Tina Wolfson, California Bar No. 174806
**AHDOOT & WOLFSON, PC**
10728 Lindbrook Drive
Los Angeles, CA 90024
Tel: (310) 474-9111
Fax: (310) 474-8585
twolfson@ahdootwolfson.com

Cornelius P. Dukelow, Oklahoma Bar No. 19086
**ABINGTON COLE + ELLERY**
320 South Boston Avenue
Suite 1130
Tulsa, Oklahoma 74103
918.588.3400 (*telephone & facsimile*)
cdukelow@abingtonlaw.com

Benjamin F. Johns, Pennsylvania Bar No. 201373
Andrew W. Ferich, Pennsylvania Bar No. 313696
**CHIMICLES SCHWARTZ KRINER**
**& DONALDSON-SMITH LLP**
One Haverford Centre
361 Lancaster Avenue
Haverford, Pennsylvania 19041
610.642.8500
bfj@chimicles.com
awf@chimicles.com

*Attorneys for Plaintiffs and the Proposed Classes*

**UNITED STATES DISTRICT COURT**
**FOR THE SOUTHERN DISTRICT OF CALIFORNIA**

VICKI STASI, SHANE WHITE, and CRYSTAL GARCIA, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

INMEDIATA HEALTH GROUP CORP.; and DOES 1 through 20, inclusive,

Defendants.

Case No. **'19CV2353 JM LL**

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs, Vicki Stasi, Shane White, and Crystal Garcia ("Plaintiffs"), on behalf of themselves individually and on behalf of all others similarly situated, allege on personal knowledge, investigation of counsel, and on information and belief as follows:

## BRIEF SUMMARY OF THE CASE

1. In January of 2019, Inmediata Health Group Corp. ("Inmediata" or "Defendant") first learned that it was experiencing a large data security incident (the "Inmediata Data Security Incident") resulting in the exposure of personal information of approximately 1,565,338 individuals ("Affected Individuals").

2. Even though Inmediata was storing sensitive personal information that it knew was valuable to criminals, and vulnerable to exfiltration, Inmediata failed to take security precautions necessary to protect Affected Individuals' data. Because Inmediata failed to take necessary security precautions, Affected Individuals' data was viewable online and downloadable. Additionally, due to a webpage setting that permitted search engines to index internal webpages that Inmediata uses for business operations, Affected Individuals' data was also searchable, findable, viewable, and downloadable by anyone with access to an internet search engine such as Google, Yahoo, Bing, etc.

3. The Affected Individuals' data exposed by Inmediata included the types of information that federal and state law requires companies to take security measures to protect: names, addresses, Social Security numbers, dates of birth, gender, and medical claim information including dates of service, diagnosis codes, procedure codes and treating physicians ("Personal Information"). This data should have received the most rigorous protection available – it did not.

## PARTIES

4. Plaintiff Vicki Stasi is an individual residing in Seminole, Florida. Inmediata received and collected Ms. Stasi's Personal Information, which Inmediata maintained in its computer systems. At the end of April, 2019, Ms. Stasi received a letter dated April 22, 2019, from Inmediata informing her that her Personal Information

may have been compromised as a result of the Inmediata Data Security Incident. Ms. Stasi now engages in monthly monitoring of her credit reports and weekly monitoring of her credit cards and bank accounts. Ms. Stasi also received an improperly addressed letter for another individual affected by the Inmediata Data Security Incident – the improperly addressed letter included Ms. Stasi's address, but the name of an individual not residing at Ms. Stasi's address. Ms. Stasi has spent approximately 20 hours of her own time attempting to determine how she is connected to Inmediata, how her information came into the possession of Inmediata, and trying to make sure she has not and does not become victimized because of the Inmediata Data Security Incident.

5. Plaintiff Shane White is an individual residing in Moorhead, Minnesota. Inmediata received and collected Mr. White's Personal Information, which Inmediata maintained in its computer systems. In approximately late April of 2019, Mr. White received a letter dated April 22, 2019, from Inmediata informing him that his Personal Information may have been compromised as a result of the Inmediata Data Security Incident. Mr. White has spent approximately 2 hours of his own time attempting to determine how he is connected to Inmediata and how his information came into the possession of Inmediata.

6. Plaintiff Crystal Garcia is an individual residing in Poway, California. Inmediata received and collected Ms. Garcia's Personal Information, which Inmediata maintained in its computer systems. In April of 2019, Ms. Garcia received a letter dated April 22, 2019, from Inmediata informing her that her Personal Information may have been compromised as a result of the Inmediata Data Security Incident. After being notified of the breach, Ms. Garcia placed credit freezes on her credit reports with the three major U.S. consumer credit reporting agencies in order to detect potential identity theft and fraudulent activity. Ms. Garcia now engages in monthly monitoring of her credit and her bank accounts. As a result of the Inmediata Data Security Incident, Ms. Garcia has spent her own money and numerous hours addressing issues arising from the Inmediata Data Security Incident. Etc.

7. Defendant Inmediata Health Group Corp. is a Puerto Rico corporation with its principal place of business and headquarters in San Juan, Puerto Rico.

## JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d) because the amount in controversy exceeds $5,000,000 (exclusive of interests and costs), because there are more than 100 members in each of the proposed classes, and because at least one member of each of the proposed classes is a citizen of a State different from Defendant.

9. This Court has personal jurisdiction over Defendant because it regularly conducts business in California.

10. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in, was directed to, and/or emanated from this District.

## STATEMENT OF FACTS

11. Inmediata is a Health Care Clearinghouse as defined by 42 U.S.C. § 1320d and provides a variety of software and service solutions to healthcare providers.

12. Inmediata's service solutions include SecureValue, SecureAlly, and SecureAR. SecureValue is an aggregator of clinical and financial data for patients from a variety of sources, including claim, electronic health record, lab, pharmacy, hospital and other data sources. SecureAlly is a cloud-based business process outsourcing solution for claims adjudication. SecureAR is an accounts receivable solution.

13. Inmediata's software solutions include SecureTrack and SecureClaim. SecureTrack is a full featured clearinghouse solution that integrates with practice management systems and electronic health record solutions. SecureTrack supports multiple specialty types including medical, dental, allied health, ambulance, and hospitals. SecureTrack supports billing for professional, dental, and institutional claims. SecureClaim is a practice management solution that integrates with clearinghouse and electronic health record solutions. SecureClaim supports multiple

specialty types including medical, dental, allied health and ambulance. SecureClaim supports billing for professional, dental, and institutional claims.

14. On or about April 24, 2019, Inmediata publicly admitted via a press release that: "In January 2019, Inmediata became aware that some electronic health information was viewable online due to a webpage setting that permitted search engines to index internal webpages that are used for business operations." https://portal.inmediata.com/patients-of-data-security-incident/ (last visited July 23, 2019).

15. In approximately April of 2019, Inmediata began filing with various state Attorneys General sample "Notice of Data Security Incident" letters that mirrored the language of the letters sent to individual consumers (including Plaintiffs). The California sample letters are attached hereto as Exhibit A.

16. The notice explained that "[i]n January 2019, Inmediata became aware that some of its member patients' electronic patient health information was publicly available online as a result of a webpage setting that permitted search engines to index pages that are part of an internal website we use for our business operations."

17. The notice further explained that "information potentially impacted by this incident may have included your name, address, date of birth, gender, and medical claim information including dates of service, diagnosis codes, procedure codes and treating physician."

18. Inmediata's notice acknowledged the very real threat that the incident would result in identity theft, fraud, and other similar risks by further informing recipients of the notice—such as Plaintiffs— to "remain vigilant by reviewing your account statements and credit reports closely."

19. Inmediata's notice also instructed victims to "promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC)."

20. Notably, Inmediata did not and has not offered or provided to the victims any fraud insurance to date. Furthermore, to date, Inmediata has only offered or provided identity monitoring services to victims who had their Social Security Numbers disclosed. Instead, Inmediata merely provided some victims with contact information for Experian, Transunion, and Equifax as well as for the Federal Trade Commission-Consumer Response Center. Inmediata made general suggestions to contact local authorities and police, in addition to suggestions on implementing a credit freeze if necessary. Essentially, all of these steps are mandated generalities used by virtually every company when publishing alerts about data security breaches. Inmediata failed to make any additional effort to mitigate or remediate the damage caused by its failure to protect sensitive personal and medical information.

21. Inmediata's own statements confirm that the Plaintiffs and the Class Members are subject to continued, future risk of identity theft, fraudulent charges and other damages. For instance, Inmediata warned consumers "remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC)."

22. A breach report filed with the Secretary of the U.S. Department of Health and Human Services on May 7, 2019, states that 1,565,338 individuals were affected by the Inmediata Data Security Incident. The May 7, 2019, filing characterizes the breach type as an "unauthorized access/disclosure" and further indicates that the breached information was located on a "network server".

23. Although Inmediata knew of the Inmediata Data Security Incident no later than January of 2019, Inmediata took no steps to notify patients whose information was affected until April 22, 2019, when Inmediata began mailing notification letters to the

potentially affected individuals directly and until April 24, 2019, via a post on Inmediata's website.

24. Inmediata had obligations created by HIPAA, and based on industry standards, to keep the compromised Personal Information confidential and to protect it from unauthorized disclosures. Plaintiffs and Class Members provided their Personal Information to Inmediata's clients with the common sense understanding that Inmediata's clients and any business partners to whom Inmediata's clients disclosed the Personal Information (i.e., Inmediata) would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

25. Inmediata acknowledges that it is subject to HIPAA. Inmediata states that it provides "[i]ndustry leading security with our data safely stored in the cloud", and that it is "[c]ompliant with HIPAA, CMS and ONC requirements". <https://portal.inmediata.com/about-us/> (last visited July 23, 2019).

26. Inmediata's data security obligations and promises were particularly important given the substantial increase in data breaches — particularly those in the healthcare industry — preceding January 2019, which were widely known to the public and to anyone in Inmediata's industries.

27. Inmediata's security failures demonstrate that it failed to honor its duties and promises by not:

a. Maintaining an adequate data security system to reduce the risk of data leaks, data breaches, and cyber-attacks;

b. Adequately protecting Plaintiffs' and Class Members' Personal Information;

c. Ensuring the confidentiality and integrity of electronic protected health information it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. Implementing technical policies and procedures for electronic information systems that maintain electronic protected health information to allow

access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

e. Implementing policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. Implementing procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. Protecting against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. § 164.306(a)(2);

h. Protecting against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

i. Ensuring compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4); and/or

j. Training all members of its workforce effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

**It is Well Established That Data Breaches Lead to Identity Theft**

28. Plaintiffs and other Class Members have been injured by the disclosure of their Personal Information in the Inmediata Data Security Incident.

29. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits and

incur charges and credit in a person's name.[1] As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

30. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[2]

31. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

32. There may be a time lag between when sensitive personal information is stolen and when it is used. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, *stolen data may be held for up to a year or more before being used to commit identity theft*. Further, once stolen data have been sold or posted on the Web, *fraudulent use of that information may continue for years*. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[3]

33. With access to an individual's Personal Information, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In

---

[1] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government Accountability Office, *available at* <https://www.gao.gov/new.items/d07737.pdf> (last visited July 23, 2019).
[2] *Id.* at 2, 9.
[3] *Id*. at 29 (emphasis added).

addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[4]

34. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, SSNs, and other Personal Information directly on various Internet websites making the information publicly available.

35. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[5] Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

36. Medical databases are especially valuable to identity thieves. According to a 2012 Nationwide Insurance report, "[a] stolen medical identity has a $50 street value – whereas a stolen social security number, on the other hand, only sells for $1."[6] In fact, the medical industry has experienced disproportionally higher instances of computer theft than any other industry.

37. To date, Inmediata does not appear to be taking any measures to assist many affected Plaintiffs and Class Members other than telling them to simply do the following:

---

[4] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, *available at* https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited July 23, 2019).

[5] *See* Elinor Mills, Study: Medical identity theft is costly for victims, CNET (Mar. 3, 2010), <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last visited July 23, 2019).

[6] Study: Few Aware of Medical Identity Theft Risk, Claims Journal, http://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited July 23, 2019).

- "remain vigilant";
- "review[] your account statements regularly and credit reports closely";
- "keep[] a close eye on your credit card activity";
- "promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities";
- obtain a copy of free credit reports;
- contact the FTC and/or the state Attorney General's office;
- enact a security freeze on credit files; and
- create a fraud alert.

None of these recommendations, however, require Inmediata to expend any effort to protect Plaintiffs' and Class Members' Personal Information.

38. Inmediata's failure to adequately protect Plaintiffs' and Class Members' Personal Information has resulted in Plaintiffs and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money—while Inmediata sits by and does nothing to assist those affected by the incident. Instead, as Inmediata's letter indicates, it is putting the burden on the Plaintiffs and Class Members to discover possible fraudulent activity and identity theft.

## CLASS ALLEGATIONS

39. Plaintiffs bring this class action lawsuit on behalf of themselves and the proposed Class Members under Rule 23 of the Federal Rules of Civil Procedure.

40. Plaintiffs seek certification of a Nationwide Class, a California Sub-Class, a Florida Sub-Class, and a Minnesota Sub-Class defined as follows:

> Nationwide Class: All persons in the United States whose Personal Information was compromised as a result of the Inmediata Data Security Incident announced by Inmediata on or around April 24, 2019.

41. In the alternative to the Nationwide Class, Plaintiffs seek certification of the following state classes:

> California Sub-Class: All persons in the State of California whose Personal Information was compromised as a result of the Inmediata Data Security Incident announced by Inmediata on or around April 24, 2019.
>
> Florida Sub-Class: All persons in the State of Florida whose Personal Information was compromised as a result of the Inmediata Data Security Incident announced by Inmediata on or around April 24, 2019.
>
> Minnesota Sub-Class: All persons in the State of Minnesota whose Personal Information was compromised as a result of the Inmediata Data Security Incident announced by Inmediata on or around April 24, 2019.

42. Specifically excluded from the Classes are Defendant and any entities in which Defendant has a controlling interest, Defendant's agents and employees, the judge to whom this action is assigned, members of the judge's staff, and the judge's immediate family.

43. **Numerosity:** Plaintiffs do not know the exact number of Class Members, but believe the Classes comprise approximately 1.5 million individuals throughout the United States. As such, Class Members are so numerous that joinder of all members is impracticable.

44. **Commonality:** Common questions of law and fact exist and predominate over any questions affecting only individual Class Members. The common questions include:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiffs' and Class Members' Personal Information;

c. Whether Defendant failed to protect Plaintiffs' and Class Members' Personal Information properly and/or as promised;

d. Whether Defendant's computer system and data security practices used to protect Plaintiffs' and the Class Members' Personal Information violated HIPAA, federal, state and local laws, or Defendant's duties;

e. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and Class Members' Personal Information;

f. Whether Defendant violated the consumer protection statutes, data breach notification statutes, state unfair insurance practice statutes, state insurance privacy statutes, and/or state medical privacy statutes applicable to Plaintiffs and Class Members;

g. Whether Defendant failed to notify Plaintiffs and Class Members about the Inmediata Data Security Incident as soon as practical and without delay after the Inmediata Data Security Incident was discovered;

h. Whether Defendant acted negligently in failing to safeguard Plaintiffs' and Class Members' Personal Information;

i. Whether Defendant express or implied contractual obligations to protect the confidentiality of Plaintiffs' and the Class Members' Personal Information, and to have reasonable data security measures;

j. Whether Defendant's conduct described herein constitutes a breach of contract with Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

m. What equitable relief is appropriate to redress Defendant's wrongful conduct; and

n. What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by Plaintiffs and Class Members.

45. **Typicality:** Plaintiffs' claims are typical of the claims of the Class Members. Plaintiffs and Class Members were injured through Defendant's uniform misconduct and their legal claims arise from the same core practices of Defendant.

46. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the interests of the Classes, and have retained counsel competent and experienced in complex litigation and class actions. Plaintiffs have no interests antagonistic to those of the Classes, and there are no defenses unique to Plaintiffs. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Classes, and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Classes.

47. **Risks:** The proposed action meets the requirements of Fed. R. Civ. P. 23 because prosecution of separate actions by individual members of the Classes would create a risk of inconsistent or varying adjudications that would establish incompatible standards for Defendant or would be dispositive of the interests of members of the proposed Classes. Furthermore, the Inmediata Database still exists, and is still vulnerable to future attacks – one standard of conduct is needed to ensure the future safety of the Inmediata Database.

48. **Injunctive Relief:** The proposed action meets the requirements of Fed. R. Civ. P. 23(b)(2) because Defendant has acted or has refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.

49. **Predominance:** The proposed action meets the requirements of Fed. R. Civ. P. 23(b)(3) because questions of law and fact common to the Classes predominate over any questions that may affect only individual Class Members in the proposed Classes.

50. **Superiority:** The proposed action also meets the requirements of Fed. R. Civ. P. 23(b)(3) because a class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each Class Member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against Defendant. Even if it were economically feasible, requiring more than 1.5 million injured plaintiffs to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. Plaintiffs anticipate no unusual difficulties in managing this class action.

51. **Certification of Particular Issues:** In the alternative, this action may be maintained as class action with respect to particular issues, in accordance with Fed. R. Civ. P. 23(c)(4).

52. Finally, all members of the purposed Classes are readily ascertainable. Defendant has access to addresses and other contact information for members of the Classes, which can be used to identify Class Members.

## COUNT I

## NEGLIGENCE

53. Plaintiffs reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

54. This count is brought on behalf of all Classes.

55. Inmediata collected and stored the Personal Information of Plaintiffs and Class Members.

56. Inmediata knew, or should have known, of the risks inherent in collecting and storing the Personal Information of Plaintiffs and Class Members.

57. Inmediata owed duties of care to Plaintiffs and Class Members whose Personal Information had been entrusted with Inmediata.

58. Inmediata breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Personal Information.

59. Inmediata acted with wanton disregard for the security of Plaintiffs' and Class Members' Personal Information. Inmediata knew or should have known that it had inadequate computer systems and data security practices to safeguard such information, and Inmediata knew or should have known that hackers were attempting to access the Personal Information in health care databases, such as theirs.

60. A "special relationship" exists between Inmediata and the Plaintiffs and Class Members. Inmediata entered into a "special relationship" with Plaintiffs and Class Members by placing their Personal Information in the Inmediata Database – information that Plaintiffs and Class Members had been required to provide to Inmediata.

61. But for Inmediata's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

62. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Inmediata's breach of its duties. Inmediata knew or should have known that it was failing to meet its duties, and that Inmediata's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Personal Information.

63. As a direct and proximate result of Inmediata's negligent conduct, Plaintiffs and Class Members now face an increased risk of future harm.

64. As a direct and proximate result of Inmediata's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

**COUNT II**

**NEGLIGENCE *PER SE***

65. Plaintiffs reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

66. This count is brought on behalf of all Classes.

67. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Inmediata had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Personal Information.

68. Pursuant to HIPAA (42 U.S.C. § 1302d et. seq.), Inmediata had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Personal Information.

69. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Inmediata had a duty to protect the security and confidentiality of Plaintiffs' and Class Members' Personal Information.

70. Pursuant to Fla. Stat. § 501.171(2), Cal. Civ. Code § 56 *et seq.*, and Minn. Stat. §144.291 *et seq.*, Inmediata had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' Personal Information.

71. Inmediata breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d et. seq.), Gramm- Leach-Bliley Act (15 U.S.C. § 6801), Fla. Stat. § 501.171(2), Cal. Civ. Code § 56 *et seq.*, and Minn. Stat. §144.291 *et seq.* by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Personal Information.

72. Inmediata's failure to comply with applicable laws and regulations constitutes negligence *per se*.

73. But for Inmediata's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

74. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Inmediata's breach of its duties. Inmediata knew or should have known that it was failing to meet its duties, and that Inmediata's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Personal Information.

75. As a direct and proximate result of Inmediata's negligent conduct, Plaintiffs and Class Members now face an increased risk of future harm.

76. As a direct and proximate result of Inmediata's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

## COUNT III

## BREACH OF CONTRACTS TO WHICH PLAINTIFFS AND CLASS MEMBERS WERE INTENDED THIRD-PARTY BENEFICIARIES

77. Plaintiffs reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

78. Upon information and belief, Plaintiffs and Class Members are intended third-party beneficiaries of contracts entered into between Inmediata and its customers, including health plans, hospitals, IPAs, and independent physicians.

79. Upon further information and belief, these contracts and require, inter alia, that Inmediata take appropriate steps to safeguard the sensitive Personal Information entrusted to it by its customers that obtain that information from Plaintiffs and Class Members.

80. Plaintiffs and the Class Members are intended third party beneficiaries of these contracts. Under the circumstances, recognition of a right to performance by Plaintiffs and the Class Members is appropriate to effectuate the intentions of the parties

to these contracts. One or more of the parties to these contracts intended to give Plaintiffs and the Class Members the benefit of the performance promised in the contracts.

81. Inmediata breached these agreements, which directly and/or proximately caused Plaintiffs and the Class Members to suffer substantial damages.

82. Upon further information and belief, Inmediata saved (or avoided spending) a substantial sum of money by knowingly failing to comply with its contractual obligations, and continues to do so.

83. Accordingly, Plaintiffs and Class Members who have been injured are entitled to damages, restitution, and other relief in an amount to be proven at trial.

**COUNT IV**

**VIOLATION OF CALIFORNIA'S**

**CONFIDENTIALITY OF MEDICAL INFORMATION ACT**

**Cal. Civ. Code § 56 *et seq.***

84. Plaintiffs reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

85. This count is brought on behalf of the California Sub-Class.

86. Inmediata is a "Contractor" as defined by Cal. Civ. Code § 56.05(d) and/or a "Provider of Health Care" as expressed in Cal. Civ. Code § 56.06.

87. Plaintiffs and Class Members are "Patients" as defined by Cal. Civ. Code § 56.05(k).

88. The Plaintiffs' and Class Members' Personal Information that was the subject of the Inmediata Data Security Incident included "Medical Information" as defined by Cal. Civ. Code § 56.05(j).

89. In violation of California's Confidentiality of Medical Information Act, Inmediata disclosed Medical Information of Plaintiffs and Class Members without first obtaining an authorization.

90. In violation of California's Confidentiality of Medical Information Act, Inmediata intentionally shared, sold, used for marketing, or otherwise used Medical Information of Plaintiffs and Class Members for a purpose not necessary to provide health care services to Plaintiffs or Class Members.

91. In violation of California's Confidentiality of Medical Information Act, Inmediata further disclosed Medical Information regarding Plaintiffs and Class Members to persons or entities not engaged in providing direct health care services to Plaintiffs or Class Members or their providers of health care or health care service plans or insurers or self-insured employers.

92. In violation of California's Confidentiality of Medical Information Act, Inmediata created, maintained, preserved, stored, abandoned, destroyed, or disposed of Medical Information of Plaintiffs and Class Members in a manner that did not preserve the confidentiality of the information contained therein.

93. In violation of California's Confidentiality of Medical Information Act, Inmediata negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Medical Information of Plaintiffs and Class Members.

94. In violation of California's Confidentiality of Medical Information Act, Inmediata's electronic health record systems or electronic medical record systems did not protect and preserve the integrity of Plaintiffs' and Class Members' Medical Information.

95. In violation of California's Confidentiality of Medical Information Act, Inmediata negligently released confidential information and records of Plaintiffs and Class Members.

96. In violation of California's Confidentiality of Medical Information Act, Inmediata negligently disclosed Medical Information of Plaintiffs and Class Members.

97. In violation of California's Confidentiality of Medical Information Act, Inmediata knowingly and willfully obtained, disclosed, and/or used Medical Information of Plaintiffs and Class Members.

98. As a direct and proximate result of Inmediata's violation of Cal. Civ. Code § 56 *et seq*., Plaintiffs and Class Members now face an increased risk of future harm.

99. As a direct and proximate result of Inmediata's violation of Cal. Civ. Code § 56 *et seq*., Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

**COUNT V**

**VIOLATION OF THE MINNESOTA HEALTH RECORDS ACT**

**Minn. Stat. § 144.291 *et seq*.**

100. Plaintiffs reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

101. This count is brought on behalf of the Minnesota Sub-Class.

102. Inmediata is a "Patient Information Service" as defined by Minn. Stat. § 144.291(Sub-2)(h), a "Provider" as defined by Minn. Stat. § 144.291(Sub-2)(i), and/or a "Related Health Care Entity" as defined by Minn. Stat. § 144.291(Sub-2)(k).

103. Plaintiffs and Class Members are "Patients" as defined by Minn. Stat. § 144.291(Sub-2)(g).

104. The Plaintiffs' and Class Members' Personal Information that was the subject of the Inmediata Data Security Incident included "Health Records" as defined by Minn. Stat. § 144.291(Sub-2)(c).

105. The Plaintiffs' and Class Members' Personal Information that was the subject of the Inmediata Data Security Incident included "Identifying Information" as defined by Minn. Stat. § 144.291(Sub-2)(d).

106. The Plaintiffs' and Class Members' Personal Information that was the subject of the Inmediata Data Security Incident included information in an "Individually Identifiable Form" as defined by Minn. Stat. § 144.291(Sub-2)(e).

107. In violation of the Minnesota Health Records Act, Inmediata released Health Records of Plaintiffs and Class Members without first obtaining consent or authorization.

108. In violation of the Minnesota Health Records Act, Inmediata negligently or intentionally released Health Records of Plaintiffs and Class Members.

109. As a direct and proximate result of Inmediata's violation of Minn. Stat. §144.291 *et seq*., Plaintiffs and Class Members now face an increased risk of future harm.

110. As a direct and proximate result of Inmediata's violation of Minn. Stat. §144.291 *et seq*., Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

## PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and the Classes, respectfully request the Court order relief and enter judgment in their favor and against Inmediata as follows:

A. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Classes as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Classes requested herein.

B. Plaintiffs request injunctive and other equitable relief as is necessary to protect the interests of the Classes, including (i) an order prohibiting Inmediata from engaging in the wrongful and unlawful acts described herein; (ii) requiring Inmediata to protect all data collected or received through the course of their business in accordance with HIPAA regulations, the Gramm-Leach Bliley Act, other federal, state and local laws, and best practices under industry standards; (iii) requiring Inmediata to design, maintain, and test their computer systems to ensure that Personal Information in their possession is adequately secured and protected; (iv) requiring Inmediata to disclose any future data breaches in a timely and accurate manner; (v) requiring Inmediata to engage third-party security auditors as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Inmediata's systems on a periodic basis and ordering them to promptly correct any problems or issues detected by these auditors; (vi) requiring Inmediata to audit, test, and train their security personnel to run automated security monitoring, aggregating, filtering and reporting on log

information in a unified manner; (vii) requiring Inmediata to implement multi-factor authentication requirements; (viii) requiring Inmediata's employees to change their passwords on a timely and regular basis, consistent with best practices; (ix) requiring Inmediata to encrypt all Personal Information; (x) requiring Inmediata to audit, test, and train its security personnel regarding any new or modified procedures; (xi) requiring Inmediata to segment data by, among other things, creating firewalls and access controls so that if one area of Inmediata's network is compromised, hackers cannot gain access to other portions of Inmediata's systems; (xii) requiring Inmediata to purge, delete, and destroy in a reasonably secure and timely manner Personal Information no longer necessary for their provision of services; (xiii) requiring Inmediata to conduct regular database scanning and securing checks; (xiv) requiring Inmediata to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (xv) requiring Inmediata to provide lifetime credit monitoring and identity theft repair services to Class Members; and (xvi) requiring Inmediata to educate all Class Members about the threats they face as a result of the loss of their Personal Information to third parties, as well as steps Class Members must take to protect themselves.

C. A judgment awarding Plaintiffs and Class Members appropriate monetary relief, including actual damages, punitive damages, treble damages, statutory damages, exemplary damages, equitable relief, restitution, and disgorgement;

D. An order that Inmediata pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

E. Pre-judgment and post-judgment interest;

F. Attorneys' fees, expenses, and the costs of this action; and

G. All other and further relief as this Court deems necessary, just, and proper.

**JURY DEMAND**

Plaintiffs demand a trial by jury on all issues so triable.

DATED: December 9, 2019

Respectfully submitted,

*/s/ Tina Wolfson*

Tina Wolfson

AHDOOT & WOLFSON, PC
10728 Lindbrook Drive
Los Angeles, CA 90024
Tel: 310.474.9111
Fax: 310.474.8585
twolfson@ahdootwolfson.com

and

Cornelius P. Dukelow*
Oklahoma Bar No. 19086
ABINGTON COLE + ELLERY
320 South Boston Avenue
Suite 1130
Tulsa, Oklahoma 74103
918.588.3400 (*telephone & facsimile*)
cdukelow@abingtonlaw.com

and

Benjamin F. Johns*
Pennsylvania Bar No. 201373
Andrew W. Ferich*
Pennsylvania Bar No. 313696
CHIMICLES SCHWARTZ KRINER
& DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, Pennsylvania 19041
610.642.8500
bfj@chimicles.com
awf@chimicles.com

**Pro Hac Vice* application to be submitted

*Counsel to Plaintiffs and the Proposed Classes*